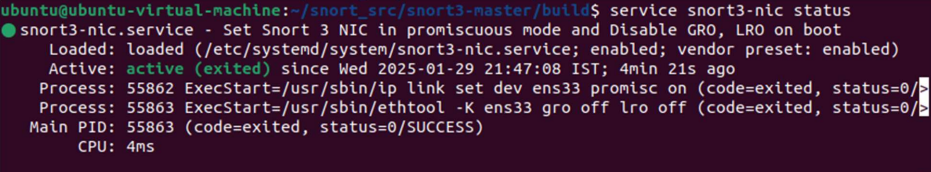
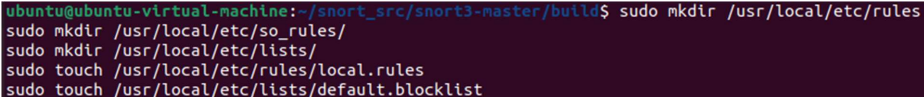
**Assignment – 6: Snort Rules**

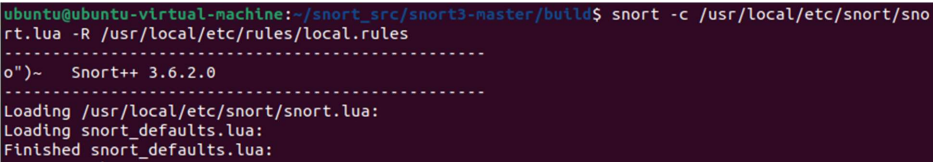
1) Install Snot and make sure it is running



2) Create folders and files

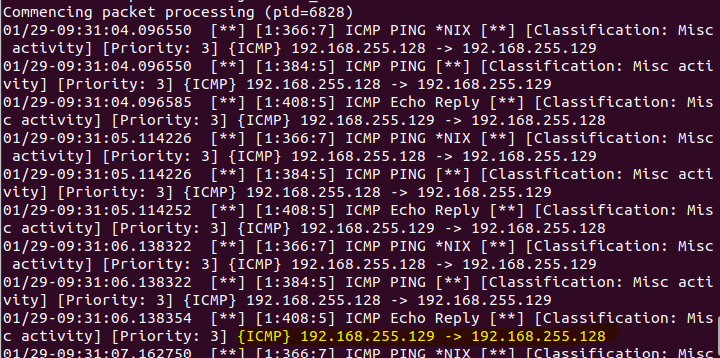


1. add a rule which detects ICMP traƯic in the local.rules file and Snort and have it load the local.rules file (using the -R parameter)



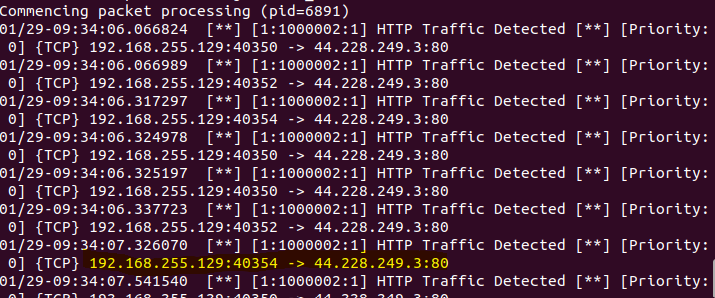
Generate ICMP traffic (e.g., by using the ping command), and verify that the alert

is triggered.



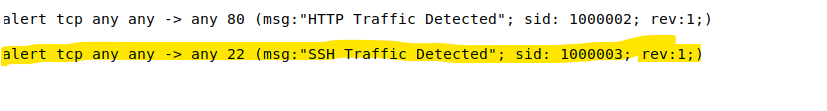
Edit the local.rules file to add a rule for capturing HTTP traffic and Open a browser and visit an HTTP website.

Run Snort in NIDS mode again using the same command. Observe the console for alerts indicating HTTP traffic.



**Extra Rules configured in Snort:**

Edit the local.rules file to add a rule for capturing SSH traffic



Run Snort in NIDS mode again using the same command. Observe the console for alerts indicating SSH traffic.

